UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/499,736	02/08/2000	Pierre Calvez	T2147-906343	1674

7590 11/10/2003

Miles & Stockbridge PC.
1751 Pinnacle Drive
Suite 500
Mclean, VA 22102-3833

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/499,736	CALVEZ ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 February 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-28 and 31-35* is/are rejected.

7)☒ Claim(s) *29 and 30* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☒ The proposed drawing correction filed on *31 May 2000* is: a)☒ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *6* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. The IDS of 2/8/2000 has been received and considered.

2. The proposed drawing corrections, filed on 5/31/2000, have been accepted.

3. The pre-amendment, filed on 5/31/2000, has been received and considered.

4. Claims 1-14 have been cancelled in their entirety, as per applicant's request.

5. Claims 15-35 are pending.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claims 15-18, 27, 28 & 32 are rejected under 35 U.S.C. 102(b) as being anticipated by the SKID protocol, described in Applied Cryptography, Second Edition, by Bruce Schneier, published 1996.

Regarding claims 15, 27 & 28, in describing various authentication protocols, Schneier discloses Alice being a user/local machine and Bob being a host/server (see page 52, 1st paragraph and page 55, 1st paragraph). Schneier discloses creating a challenge/random number and communicating it along with elements known by the user/"A" to the server/"B" (see page 55, step 1 and page 56, step 3). Schneier discloses performing a calculation/hash, obtaining a first response/R_B,$H_k(R_A,R_B,B)$ and transmitting that response (see page 55, step 2) to the user/"A". Schneier discloses performing a second calculation/hash that is a function of predetermined data and comparing the results (see page 56, step 3).

Regarding claims 16, 17 & 18, Schneier discloses a hash being performed over the challenge/random number (see page 55, step 2 and page 55, step 3).

Regarding claim 32, Schneier discloses a response/$H_k(R_A,R_B,B)$ composed of hashing a string composed of a fixed security key/K stored in the local machine/B and server/A, the name of the local machine/B (see page 55, step 2).

8. Claim 35 is rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,161,185 to Guthrie et al. (Guthrie). Guthrie discloses a user (Fig. 5, element 114), local machine (Fig. 5, element 102) and remote server (Fig. 5, element 104), means for classifying

information (Fig. 5, element 120) and communication means (Fig. 5, element 112 & 118). Guthrie further discloses a system administrator (see col. 2, lines 42-47), a local machine comprising an authentication module that include a first user module (Fig. 5, element 126) for generating a challenge (Fig. 4, element 114) and second user module for generating a response (Fig. 5, element 130) and an administrative authentication module for authorizing access (Fig. 5, element 132).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 19-23 & 31 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a), as applied to claims 16, 17 & 18 above, as obvious over Applied Cryptography, Second Edition, by Bruce Schneier.

Regarding claims 19, 20 & 21, Schneier discloses the SKID protocol, as described above, but the protocol lacks sharing a secret value. However, Schneier teaches that "In general, a man-in-the-middle attack can defeat any protocol that doesn't involve a secret of some kind." Schneier further teaches that protocols that combine authentication with key exchange solve a general computer problem wherein different users want to communicate securely (see page 56, 2nd paragraph). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish a secret key between the local machine and server

to enable secure communication after authentication. One of ordinary skill in the art would have been motivated to perform such a modification to enable secure communication and to secure the transaction from the man-in-the-middle attack, as taught by Schneier.

Regarding claim 22, Schneier discloses the SKID protocol, as described above, but lacks modifying a shared secret with a key that depends on the local machine. However, in a discussion of key-exchange protocols, Schneier discloses that public key cryptography makes key exchange easier, in that a first party encrypts a secret with the public key of a second party. This allows only the second party access to the secret (see page 48). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the shared secret with a key that depends on the local machine to make key exchange easier. One of ordinary skill in the art would have been motivated to perform such a modification to make key exchange easier, as taught by Schneier.

Regarding claim 23, Schneier discloses a byte string consisting of hashing a Master Station Secret/R_A to obtain a Station Secret/$H_k(R_A,R_B,B)$ (see page 55, step 2).

Regarding claim 31, Schneier discloses a response/$H_k(R_A,R_B,B)$ composed of hashing a string composed of a user's password/K, a Station Secret/R_A and the user name/B (see page 55, step 2).

11. Claims 24, 25 & 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, as applied to claims 16, 17 & 18 above, in view of U.S. Patent 5,081,677 to Green et al. (Green). Schneier discloses an authentication protocol, as described above, but lacks a version number associated with a shared secret, and incremented when the shared secret is

modified. However, Green teaches that, when updating a master key, it is useful to associate a version number with a the key and to increment the version number when the key is modified, to enable distributed copies of the key to be updated on first use and to modify the master key without exposing it to applications (see col. 2, lines 30-67 and col. 3, lines 5-35). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to associate a version number with a shared secret and to increment the version number when the secret is modified. One of ordinary skill in the art would have been motivated to perform such a modification to enable the shared secrets to be updated at different times (on first use) and to enable modification of the secret without exposing it, as taught by Green.

12. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, as applied to claim 15 above, in view of U.S. Patent 5,774,650 to Chapman et al. (Chapman). Schneier discloses an authentication protocol, as described above, but lacks temporary authorization where the duration is configurable. Chapman teaches time-limited access to a system is beneficial to temporarily enable a privileged user to use the full performance capability of a system by temporarily denying access to less-privileged users (see col. 2, lines 38-61). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a time-based authorization in Schneier's system to enable a privileged user to access the full capabilities of the system. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of enabling a user to temporarily gain full access to a system's resources.

13. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, as applied to claim 15 above, in view of Windows NT User Administration, by Ashley J. Meggitt & Timothy D. Ritchey (Meggitt). Schneier discloses an authentication protocol, as described above, but lacks specific disclosure of locally authenticating a user after disconnection. However, Meggitt teaches that Windows NT allows a user, normally authenticated through a domain, to login to a local workstation even if the roaming profile is unavailable. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the authentication protocol taught by Schneier to allow login to a local machine by a user, usually authenticated remotely, in the case that network connectivity has been disrupted. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of local system access even when remote authentication is unavailable, as taught by Meggitt.

Allowable Subject Matter

14. Claims 29 & 30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

15. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 29 & 30, the prior art relied upon fails to specifically teach the limitation of a challenge composed of a first byte representing the type of challenge, the type of challenge indicating whether a network authentication has been performed; second and third

bytes representing the version number of the shared information; and random alphanumeric characters of the fourth to twelfth bytes.

Conclusion

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:30 p.m.. The examiner can also be reached on alternate Fridays from 8:00 a.m. – 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

MJS
30 October 2003

NORMAN M. WRIGHT
PRIMARY EXAMINER